

Medical Practice Compliance

News, tools and best practices
to assess risk and protect physicians

ALERT

July 13, 2009 | Vol. 21, Issue 13

IN THIS ISSUE

Interest overcharges raise compliance risks	1
5 steps to deal with closer scrutiny of payer relationships	1
Make the case for internal audits in a tight economy	2
5 questions you must answer when you audit your infusion claims	3
3 lessons you can learn from Allina	3
Private payer contracts crackdown put you in the crosshairs	4
Fraud bust, OIG audit target infusion services	4
From the DecisionHealth Professional Services case files	6
From the Compliance Toolbox	8

Interest overcharges raise compliance risks

Add this to your compliance to-do list: Make sure the interest rate you charge patients is in compliance with your state's usury laws. When you charge more than you're legally allowed, you can end up with a compliance problem.

More patients than ever are struggling financially with their medical bills and paying in installments over time, according to David Kanihan, spokesperson for Allina Hospitals and Clinics in Minneapolis. As a result, more providers are charging interest on unpaid balances and have a higher percentage of patients paying interest than in previous years.

"This has gotten more important to deal with," Kanihan points out.

However, Allina was cited for allegedly charging more interest to patients than allowed under Minnesota law – at least according to the state's Attorney General's office. Allina and the attorney general signed an agreement settling a lawsuit filed by the state relating to interest charged to users of MedCredit, Allina's consumer medical financing program. *(continued on page 4)*

5 steps to deal with closer scrutiny of payer relationships

The government has begun to crack down on private payers who commit Medicare and/or Medicaid fraud and providers who partner with these payers may end up in the government's crosshairs (see story, pg. 4).

Take these five steps to protect yourself:

1. **Comply with all rules and regulations.** You aren't immune because you only treat the patients of the payer. You can defend yourself much more easily when the government scrutinizes the payer network by proving you follow the law. **Example:** You can be accused of helping a Medicare or Medicaid capitation or risk-based plan manipulate the program to increase payments, warns attorney Tina Dunsford, with Foley & Lardner in Tampa. You can also be turned in by the payer or a whistleblower who believes you're submitting false claims, she adds. *(continued on page 5)*

Make the case for internal audits in a tight economy

Don't let people in your practice use the weak economy as a reason to put your compliance audits on the back burner.

You know regular audits are essential to your compliance program, but the word "audit" is loaded with negative connotations. Clinicians picture a grim payer official hunting for mistakes and demanding a big check to cover overpayments. Convince reluctant providers that internal audits protect your practice with these four examples of how failure to follow a regular audit policy can result in a hit to a practice's bottom line:

1. Missed audits are missed opportunities: A good internal audit helps you pinpoint money your clinicians are leaving on the table, says Curt Udell, compliance & privacy officer for Premier Physician Group, multispecialty practice in Bethesda, Md. Udell believes this is particularly true for primary care physicians and surgeons. Objections to the cost of an audit aren't a valid argument, Udell says. Even if you bring in an outside consultant to conduct a full audit, the cost should not be more than one day's work for a primary care physician or one surgical procedure for a surgeon, Udell says.

2. Lost stars and lost patients: United Health-Care (UHC) uses a two-star rating system for its doctors

and shares that information with patients. UHC doesn't notify the doctor when it determines or changes his or her ranking, says Maxine Lewis CPC, president of Medical Coding Reimbursement Management in Cincinnati. A two-star physician lost a star because he coded every patient as being chronically ill. He started losing patients to two-star doctors, but UHC would not restore his second star unless he allowed the payer to conduct a full audit. Regular internal audits would have caught and corrected his coding mistakes, Lewis says, allowing him to keep both of his stars and his patients.

3. Minor external audits can escalate: If you treat patients enrolled in Medicare Advantage plans, a plan can request charts it will review to determine their patient groups' severity of disease. The plans use this information to gain higher payments from Medicare. However, Lewis warns, if the MA's auditor notices anything irregular in your claims, the information gets passed to the plan's investigative arm.

4. Your work, other people's pay: Individual providers may be doing work while another provider gets paid. Lewis gives the example of a cardiology practice where one physician refers the patient for an EKG, a second physician reads the results, but the practice bills for the reading under the first physician's name. Not only was this improper, the reading physician wasn't getting credit or payment for his work. "They just didn't under-

Subscriber Services

Editorial:

Scott Kraft – (301) 287-2361 skraft@decisionhealth.com
 Marla Durben Hirsch – (301) 299-6155 mhirsch@decisionhealth.com
 Julia Kyles – (301) 287-2651 jkyles@decisionhealth.com
 Sean Weiss – vice president DecisionHealth Professional Services
sweiss@dhprofessionalservices.com

Marketing:

Elise Yore – (301) 287-2274 eyore@decisionhealth.com

Subscriptions:

For direct questions about newsletter delivery and account status, please contact DecisionHealth® at (877) 602-3835, or email us at: customer@decisionhealth.com

Compliance Listserv:

To join our free Internet forum on fraud and abuse issues, go to <http://listserv.ucg.com/cgi-bin/listserv/listserv.pl/fraud-l>, click on the "Join the Fraud & Abuse Discussion Group" link, and follow the instructions.

Reprints:

To request permission to make photocopy reprints of *Medical Practice Compliance Alert* articles, or to obtain information on our copyright waiver, multiple copy and site license programs, please call us at (866) 266-1029, or email Joe Wethje at: jwethje@decisionhealth.com.

How You Can Redistribute MPCA?

It is illegal to photocopy or electronically forward any part of **Medical Practice Compliance Alert** in paper or electronic form to anyone without our permission. It violates our copyright. But we understand that part of your job is to help educate and train others on how to comply with complex Medicare and Medicaid rules. The ability to share *MPCA* with staff members could be a key component of that effort, saving you a huge amount of time and money. That's why we offer a special, customized license to redistribute each issue. For more information, contact Julia Kyles at (301) 287-2651 or jkyles@decisionhealth.com. In the meantime, if you received **Medical Practice Compliance Alert** and you are not the named subscriber, it is a violation of federal copyright law. However, only the party that provides the copyrighted material is at risk, not you. To confidentially report suspected copyright violations, call our copyright attorney Roger Klein at 202-383-6846 or email him at KleinR@howrey.com. Copyright violations will be prosecuted. And **Medical Practice Compliance Alert** shares 10% of the net proceeds of settlements or jury awards with individuals who provide essential evidence of illegal photocopying or electronic forwarding of our newsletter.

Medical Practice Compliance Alert is published 24 times per year by:

DecisionHealth® (a UCG company)
 Two Washingtonian Center
 9737 Washingtonian Blvd., Suite 100
 Gaithersburg, MD 20878-7364

ISSN: 1047-1863
Price: \$539 per year
 DecisionHealth® is a registered trademark of UCG

stand the rules,” Lewis says, but regular audits would have caught the mistake.

Note: Physicians need to be aware that Medicare’s carriers aren’t the only payers looking to recoup overpayments, Lewis warns. Private payers, Medicaid, even employer pension plans are all ramping up their audit activity to counter their own financial stresses. And don’t forget the Recovery Audit Contractors (RACs), Udell cautions. These audits won’t be random, he says. “They’ll use high-tech data mining techniques to find overpayments and any irregularities will bubble to the top.”

“Nobody likes to be audited, but if you do it correctly, physicians and patients will benefit and the RACs will be stymied,” Udell says.

5 questions you must answer when you audit infusion claims

When you review your infusion claims, make sure you can answer these five questions. If you can’t, your claims are much more likely to catch extra scrutiny and lead to repayment demands during an audit.

1. **Does the treatment make sense?** The patient’s diagnosis and treatment should match the protocol for use of the drug including length of treatment and dosage size, says Julie Urda CPC, president of ProActive Billing and Management Services in San Diego. Example: The doctor determines the patient has a staph infection that requires infusion therapy. The course of treatment usually lasts four to six weeks. Any reason for the treatment to go beyond that should be documented in the chart with a certificate of medical necessity and a treatment plan signed by the doctor, Urda says.

TIP Submit documentation to private payers with the claim to avoid payment delay, Urda says. She is seeing more requests for medical records for infusion therapy treatment.

2. **Did you follow your carrier’s rules for chemo billing?** Carriers have leeway to decide what drugs qualify as chemotherapy, says Lawrence Martinelli, MD of Consultants in Infectious Diseases, a three-doctor practice in Lubbock, Texas. Example: One carrier may classify Epogen as chemotherapy while another may deem it therapeutic.

3. **What was the initial service?** You can only bill one initial infusion service a day, notes Martinelli. Example: If the patient receives chemotherapy and hydration therapy on the same day, you can only bill one of those

3 lessons you can learn from Allina

Stay on top of the law if you want to charge and collect interest from patients (see story, pg. 1). To protect yourself, you must:

1. **Check that the interest rate you’re charging is within the law.** State usury laws vary widely. Check on the Internet or ask your attorney general’s office. Get advice from someone knowledgeable about finance law if you’re not familiar with your state’s law, says a former Allina employee familiar with the situation.

2. **Make sure you’re in compliance with state and federal laws. Example:** Both Minnesota and the federal Truth in Lending Act require providers to notify patients before treatment that they may be charged interest. Allina has that notification in its registration form.

3. **Work with the government to solve the problem.** Once the attorney general brought the matter to Allina’s attention, Allina took a collaborative approach to resolve the problem, and agreed to lower the interest rate, even though it believed it was acting lawfully, says Allina spokesperson David Kanihan.

services as an initial hour, Martinelli explains. Choose the initial service based on the primary reason the patient is in the office that day.

4. **Did you double bill?** Accidental double billing of a private payer is fairly common, says Gary Collins, president of Professional Reimbursement Inc., in Orlando, Fla. Example: The doctor bills the carrier. The carrier denies the claim, but electronically crosses it over to a secondary payer. The provider sees the denial from the carrier and rather than wait, bills the secondary payer directly. When the secondary insurer pays twice, the money needs to be returned.

TIP Scrutinize Explanation of Benefits for two payments for the same patient on the same date of service at least once a month, Collins says.

5. **Is your documentation complete?** Make sure your J codes match your administration codes and clearly document the start and stop times of the therapy, Martinelli says. Your documentation should show that a doctor was in the office while the drips were running to show you’re meeting supervision requirements.

Remember: Carriers and investigators are scrutinizing these services to make sure neither fraud nor improper payments are leeching money from Medicare. Not only are enforcement officials targeting fraud that involves infusion, but your carrier and recovery audit contractors could also take a special interest in these claims (see story, pg. 4).

Private payer contracts crackdown puts your practice in crosshairs as well

Prepare for fraud problems that may come from your private payer relationships. The government has begun a crackdown on private payers who commit Medicare and Medicaid fraud. When you partner with these payers, you may end up in the government's crosshairs (see story, pg. 1).

The government has taken two more aggressive steps in its fight against health care fraud, both of which can affect you and the private payers. The first step is the joint Health Care Fraud Prevention and Enforcement Action Team (HEAT) program announced May 20 by the Departments of Justice (DOJ) and Health and Human Services (HHS) to prevent and combat Medicare fraud (MPCA 6/15/09).

One of the goals of HEAT is to strengthen activities to monitor and ensure compliance and enforcement by Medicare Advantage plans (Medicare Part C) and prescription drug programs (Medicare Part D).

On the same day that HEAT was announced, President Obama signed a new law, called the Fraud Enforcement and Recovery Act of 2009 (FERA), which makes it easier to find you liable for violating the False Claims Act (FCA) just by working with a Medicare or Medicaid managed care plan.

FERA also makes it easier for the government to claim you and a payer (or more than one provider) conspired to violate the FCA, warns attorney Fred Cohen, with Goldberg Kohn in Chicago.

Private payers are already feeling the pressure. Medicaid HMO WellCare Health Plans agreed May 5 to enter into a deferred prosecution agreement regarding allegations that it had schemed to defraud the Florida Medicaid Program by submitting inflated expenditure information. WellCare also agreed to pay \$80 million in restitution and forfeiture.

Why you should be concerned

Don't take these developments lightly. Any scrutiny of your business partners for fraud puts you at risk that investigators will turn their attention to you as well. You are far more likely to contract with Medicare and Medicaid managed care plans than less common deals such as pharmaceutical consulting arrangements. Simply getting paid by one of these plans is enough to put you on the government's radar. Even if you're innocent, you

still have to spend time and money to defend yourself.

You could also have to do so more often. Experts predict a "dramatic" increase in enforcement. "These changes are significant. It suggests that Congress intended to pay for new law enforcement resources by increased collections from more vigorous enforcement of the FCA," says attorney Judith Waltz, Foley & Lardner, in San Francisco.

There will also be an uptick in whistleblower litigation. "I expect an explosion in [these] lawsuits. It doesn't take much to file these," warns former health care fraud prosecutor Jonathan Halpern, now an attorney with Bracewell & Giuliani in New York City.

Fraud bust, OIG audit target infusion services

Make sure your infusion therapy claims are especially clean because they'll likely face extra scrutiny after a Detroit-based infusion therapy fraud investigation resulted in 53 arrests on June 24.

The three-year investigation by HHS's "Motor City Strike Force" alleges \$16 million in fraudulent billing. The HHS Office of Inspector General (OIG) also noted in a recent report that more than \$60 million in claims for chemotherapy services could not be matched to a qualifying drug.

OIG suggested that all carriers conduct probe audits of chemotherapy claims and noted that Recovery Audit Contractors (RACs) have also expressed an interest in reviewing these claims. For six tips on what you should look for during an audit, see the story on pg. 3.

On the Internet:

- ▶ Motor City Strike Force Press Release: <http://www.hhs.gov/news/press/2009pres/06/20090624a.html>
- ▶ OIG Inspection Report – Medicare Part B chemotherapy Administration: Payment & policy: <http://www.oig.hhs.gov/oei/reports/oei-09-08-00190.pdf>

Interest overcharges

(continued from page 1)

Allina will be required to reimburse patients who were allegedly overcharged, according to terms of the settlement. Allina will have to pay back at least \$1.1 million, which covers thousands of patients, according to Allina.

Allina disputes that it overcharged patients. There are

two types of arrangements in Minnesota where providers can charge patients interest. For general debtor installment agreements, the interest rate is 8% (the rate is 6% interest without a special agreement or arrangement). But providers can also implement an open-ended credit program, such as Allina's MedCredit program, which allows patients to have an ongoing account and pay their medical debt over time, according to a former employee familiar with the situation.

MedCredit had been operating for a "long time" and provided these services to other Minnesota providers, says Kanihan.

"It's a credit transaction, like a credit card, with no cap on the interest rate. It's like having an unsecured loan for health care debt without having to go through a background check. [MedCredit] charged on a sliding scale up to 18%," he says.

Allina argued that it was entitled to charge the higher rate under the MedCredit program. The attorney general disagreed, saying that Allina was only allowed to charge up to 8%, although Attorney General Lori Swanson acknowledged in her press release announcing the settlement that providers "are facing their own financial pressures as a result of the bad economy and lack of adequate insurance coverage for patients." The attorney general's office did not respond to **Medical Practice Compliance Alert's** requests for additional comment.

This issue will pick up speed, especially with the current economic environment and the increased focus on health care costs.

"It gave the Attorney General some nice headlines. And with the incredible rise in self pay debt and more people out of work, patients will be looking for solutions to pay their [medical] debt," the insider points out.

5 Steps

(continued from page 1)

2. Review fraud or other settlements of your payers to measure your compliance risk. A settlement agreement involving the payer's inappropriate marketing doesn't create a large compliance risk on a provider, notes attorney Rick Robinson, with Fulbright & Jaworski, Washington, D.C. But if the payer agrees to be excluded from Medicare, your compliance risk is increased because you're contracting with an excluded entity, points out Robinson.

3. Decide whether you want to remain partners

with a payer settling with the government. This will depend in part on what the payer got in trouble for, its patient base and your view of yourself as a provider, says attorney Fred Cohen, with Goldberg Kohn in Chicago. You can presume that the payer will be compliant going forward, because the government has its eye on the payer, but you may also decide you don't want to be associated with the payer anymore, notes Cohen.

4. Review your contract before terminating it. Check your contract to see what options you may have to terminate when you decide to sever a relationship. The contract likely dictates how you can end the contract and may allow you to terminate more quickly "for cause," says Cohen.

5. Keep an eye out for whether the payer is running into financial trouble. Many payers intend to stay in business after a government investigation, but administrative cost increases from legal issues could push the payer into receivership or insolvency, warns Dunsford. You may get paid only pennies on the dollar at most in these cases, and may not be able to terminate the contract until a court lets you do so. When a payer takes longer to pay or suddenly denies larger claims, follow up with the payer to protect yourself, she suggests.

Protect your practice from compliance risks

To protect your practice from audits, investigations and even accusations of fraud, you must keep up with the latest compliance requirements. Take advantage of these up-coming training opportunities that you and your staff can attend without leaving the office. For more information call 1-866-620-5939 or go to www.decision-health.com and click "EVENTS":

HIPAA & Red Flag Rules: You've got more responsibilities than ever when it comes to keeping your patients' information safe. A failure to take the proper steps at the right time can expose your practice to hefty fines and bad press. Make sure you're ready by tuning in to the **Who let the healthcare data out? 10 steps to handle a security breach** audio conference on Aug. 12, 1 – 2:30 p.m.

Medicare's regulations: Scribes can make your doctors' lives easier, but if you don't follow Medicare's rules, you could wind up in the midst of an investigation. Get tips for using scribes correctly during the **Scribes: How to comply with Medicare's rules & avoid penalties** audio conference on Aug. 18, 1 – 2: 30 p.m.



From the
DECISIONHEALTH® PROFESSIONAL SERVICES
Case Files

Case #14: The Case of the Misused Modifier

The client: A solo physician practice located in the Southeast.

The audit: DecisionHealth Professional Services came in to assess how coding and documentation errors were leading to revenue shortfalls.

The compliance risk: The doctor was using modifier **59** (distinct procedural service) far more frequently than could be justified by the documentation for the services provided.

Background:

Modifiers give the payer additional information beyond the code itself about the services provided and can also lead to higher payments when used appropriately. However, when used inappropriately they can cost the practice money through lost revenue opportunities and denials, overpayment demands and pre-payment review.

When an auditor or investigator believes the incorrect use of modifiers rises to the level of abuse or fraud, it can create legal headaches for providers forced to spend a lot of time and money responding to an investigation.

According to CMS, Modifier 59 "... is used to indicate that a provider performed a **distinct** procedure or service for a beneficiary on the same day as another procedure or service. It may represent a different session, different procedure or surgery, different anatomical site or organ system, separate incision or excision."

The misuse of modifier 59 is particularly troubling because there's so much information about the correct use readily available.

The HHS Office of Inspector General's (OIG's) Office of Evaluations & Inspections found misuse of this modifier was a widespread problem almost four years ago. OIG released its findings in a report titled "Use of Modifier 59 to Bypass Medicare's National Correct Coding Initiative Edits."

According to OIG, modifier 59 was billed improperly 40% of the time in 2003, the year surveyed, resulting in \$59 million in improper payments. Here's a breakdown of what OIG found:

- Modifier 59 was used inappropriately with 15% of the code pairs because the services were not distinct from each other. Secondary services are the services CCI edits would deny. Most of these services were not distinct because they were performed during the same session, at the same anatomical site and/or through the same incision as the primary service.
- Five code pairs represented 53% of the services that were not distinct:
 1. **38221** (bone marrow biopsy) and **38220** (bone marrow aspiration).
 2. **97140** (manual therapy techniques) and **97530** (therapeutic activities, direct).
 3. **88108** (cytopath concentrate) and **88104** (cytopathology, fluids).
 4. **96410** (chemo admin, IV infusion) and **90780** (IV infusion).
 5. **96408** (chemo admin, IV push) and **90780** (IV infusion).
- 25% of code pairs billed with modifier 59 were not adequately documented.

CMS and individual carriers also have posted information about the proper use of this modifier. Medicare expects providers to read and follow these instructions. The agency won't accept that you were too busy as an excuse.

The investigation:

We reviewed claims for a six month period and the corresponding documentation to support the services billed.

Case Files

(continued from page 6)

Note: When we conduct our audits we always use a CPT manual for the year that we're auditing as well as the appropriate CCI edits for the applicable quarter. What is bundled today may not have been bundled during a previous quarter, so it is critical when you perform an audit that you have the relevant tools for that period of claims submission.

We quickly noticed an abnormal number of modifier 59s. We ran a modifier report in the system and found almost 15,000 examples of this provider adding modifier 59 to subsequent procedures.

We took a closer look at the codes being "exploded" or unbundled and realized there were often other codes that could have been used to explain the combination of services performed. But, because the practice was looking to optimize their reimbursement, they chose to "explode" the codes in the categories that should have been bundled into one code.

Recommended corrective action plan:

I explained to the physician and the practice manager that an audit by CMS, a carrier, Recovery Audit Contractor or other government auditor could expose the doctor to accusations of fraud or abuse. I also gave an outline of the civil monetary or criminal

finances she could face if she were found guilty of fraud. I discussed the merits of repaying the funds before Medicare or a contractor found the problem.

Finally, I reviewed the proper use of modifier 59 and left the practice with educational material they could refer to going forward.

Editor's Note: One of the DecisionHealth Professional Services tools offered during this case is attached to the e-mail version of this week's Medical Practice Compliance Alert.

On the Internet:

- OIG's report on Modifier 59: <http://oig.hhs.gov/oei/reports/oei-03-02-00771.pdf>

Sean M. Weiss, vice president & chief compliance officer of DecisionHealth can be contacted directly at sweiss@dhprofessionalservices.com or at 770-402-0855. DecisionHealth Professional Services, is a service of DecisionHealth and provides full-scale medical consulting services in the areas of practice management, compliance and coding as well as health law services. To schedule a DecisionHealth Senior Consultant to come onsite to your practice or to learn more about our services visit us at www.dhprofessionalservices.com or contact us at 1-888-262-8354.

Have a colleague who could benefit from *Medical Practice Compliance Alert*. Pass this along!

YES! I want the latest business and regulatory news, benchmarks, best practices and executive tools for to increase my profitability and ensure agency growth. Please enter my for one year (48 issues) subscription at \$477 for *Medical Practice Compliance Alert*.

Name: _____

Org: _____

Address: _____

City:State:ZIP: _____

Phone: _____

Fax: _____

Email: _____

www.compliancealert.net

Payment enclosed. (Make checks payable to *Medical Practice Compliance Alert*; (TIN: 26-3622553)

Send me an invoice (PO _____)

Charge my:    

Card #: _____

Exp.Date: _____

Signature: _____

Mail to: **Medical Practice Compliance Alert**

Two Washingtonian Center, 9737 Washingtonian Blvd., Ste. 100,
Gaithersburg, MD 20878-7364 | 877-602-3835

PAS 2009

From the Compliance Toolbox

Medical Identity Theft Response Checklist for Consumers

This checklist was provided by and used with permission of the American Health Information Management Association (AHIMA), Chicago. It's from AHIMA's e-HIM Work Group on Medical Identity Theft Report "Mitigating Medical Identity Theft," Journal of AHIMA 79, no. 7, July 2008. You can provide the checklist to patients when it's discovered that a patient has been the victim of medical identity theft.

Note: This form is also attached to the email version of this week's Medical Practice Compliance Alert.

Activity	Done
Explore the resource "Tools for Victims" provided by the Federal Trade Commission (FTC) (www.ftc.gov/bcp/edu/microsites/idtheft/tools.html). Consider completing the universal affidavit to submit to creditors.	
Review credit reports, correct them, and place a "Fraud Alert" on them.	
If a Social Security number is suspected of being used inappropriately, contact the Social Security Administration's fraud hotline at 1-800-269-0721.	
In the case of stolen or misdirected mail, contact the US Postal Service at 1-800-275-8777 to obtain the number of the local US Postal Inspector.	
For stolen passports, contact the US Department of State at 1-877-487-2778 or http://travel.state.gov .	
If the thief has stolen checks, contact both check verification companies: Telecheck (1-800-366-2425) and the international Check Services Company (1-800-526-5380) to place a fraud alert on the account to ensure that counterfeit checks will be refused.	
Contact the health information manager or the privacy officer at the provider organization or the anti-fraud hotline at the health plan where the medical identity theft appears to have occurred.	
Request an accounting of disclosures. If the provider or plan refuses access to medical records, file a complaint with the Office for Civil Rights at Health and Human Services at 1-866-627-7748 or www.hhs.gov/ocr/privacy/howtofile.htm .	
Take detailed notes of all conversations related to the medical identity theft. Write down the date, name, and contact information of everyone contacted, as well as the content of the conversation.	
Make copies of any letters, reports, documents, and email sent or received regarding the identity theft.	
Work with the organization where the medical identity theft occurred to stop the flow of the incorrect information, correct the existing inaccurate health record entries, and determine where incorrect information was sent.	
File a police report and send copies with correct information to insurers, providers, and credit bureaus once the identity theft has been confirmed.	
File a complaint with the attorney general in the state where the theft occurred. The National Association of Attorneys General provides state-by-state information at www.naag.org/attorneys_general.php .	
Check with state authorities for resources. Many states provide consumer protection and education related to insurance and accept online complaints. To determine if a state has a state insurance department for online complaints, visit the National Association of Insurance Commissioners at www.naic.org and file a complaint as appropriate.	
File a complaint with the Identity Theft Data Clearinghouse. Information can be found at https://m.ftc.gov/pls/dod/widtpubl\$.startup?Z_ORG_CODE=PU03 .	
Contact the Department of Health and Human Services at 1-800-368-1019 or by visiting the Web site at www.hhs.gov/ocr for suspected Medicare or Medicaid fraud.	
Review health records to make sure they have been corrected prior to seeking healthcare.	
Change all personal identification numbers and passwords for protected accounts, sites, access points, etc. Choose unique personal identification numbers and complex passwords rather than common ones (e.g., mother's maiden name, birth date, or pet name).	

How did you get this email?

Copyright notice

It is illegal to forward this electronic version of **Medical Practice Compliance Alert** to anyone else. It is a free benefit only for the individual listed by name as the subscriber. It's illegal to distribute electronically **Medical Practice Compliance Alert** to others in your office or other sites affiliated with your organization. If this email has been forwarded to you and you're not the named subscriber, that is a violation of federal copyright law. However, only the party that forwards a copyrighted email is at risk, not you.

To confidentially report suspected copyright violations, call our copyright attorney Roger Klein at 202-383-6846 or email him at KleinR@howrey.com. Copyright violations will be prosecuted. And **Medical Practice Compliance Alert** shares 10% of the net proceeds of settlements or jury awards with individuals who provide essential evidence of illegal electronic forwarding of **Medical Practice Compliance Alert** or photocopying of our newsletter.